SPYWOLF

Security Audit Report

Completed on

December 30, 2022

OVERVIEW

This audit has been prepared for **GEISHA** to review the main aspects of the project to help investors make make an informative decision during their research process.

You will find a a summarized review of the following key points:

- ✔ Contract's source code
- ✔ Owners' wallets
- ✔ Tokenomics
- ✔ Team transparency and goals
- ✔ Website's age, code, security and UX
- ✔ Whitepaper and roadmap
- ✔ Social media & online presence

The results of this audit are purely based on the team's evaluation and does not guarantee nor reflect the projects outcome and goal

- SPYWOLF Team -

TABLE OF CONTENTS

GEISHA

PROJECT DESCRIPTION

According to their website/whitepaper:

Geisha is a meme token based on the "name given to women who have been accompanying male customers with songs, dances, conversations and games in the entertainment life in Japan since the 17th century. The geisha world is called Hana-machi (花街: Flower town) or Ka-ryu-kai (花柳界: Flower-willow-world) in Japanese."

Release Date: Launched in December, 2022

Category: Meme token

CONTRACT INFO

Token Name Geisha	Symbol GEISHA
Contract Address 0x54D7b47eE0BC89A94d9253234aacC69FEbEf0000	
Network Ethereum	Language Solidity
Deployment Date Dec 30, 2022	Verified? Yes
Total Supply 10,000,000 GEISHA	Status Launched

TAXES

Buy Tax	Sell Tax
3%	3%

*Taxes cannot be changed in future

Our Contract Review Process

The contract review process pays special attention to the following:

- Testing the smart contracts against both common and uncommon vulnerabilities
- Assessing the codebase to ensure compliance with current best practices and industry standards.
- Ensuring contract logic meets the specifications and intentions of the client.
- Cross referencing contract structure and implementation against similar smart contracts produced by industry leaders.
- Thorough line-by-line manual review of the entire codebase by industry experts.

Blockchain security tools used:

- OpenZeppelin
- Mythril
- Solidity Compiler
- Hardhat

TOKEN TRANSFERS STATS

Transfer Count	717
Uniq Senders	164
Uniq Receivers	284
Total Amount	61012323.61000814 GEISHA
Median Transfer Amount	40413.758046777 GEISHA
Average Transfer Amount	85093.89624826798 GEISHA
First transfer date	2022-12-30
Last transfer date	2022-12-30
Days token transferred	1

SMART CONTRACT STATS

Calls Count	2442
External calls	220
Internal calls	2222
Transactions count	899
Uniq Callers	233
Days contract called	1
Last transaction time	2022-12-30 11:38:11 UTC
Created	2022-12-30 01:34:47 UTC
Create TX	0x55b3bda71631f760c6e4ca81a315c1698f81024e9861d78a8f418e442845bce5
Creator	0xf010c756f4ea4ab1ea35823b3f42631433d9a0d3

FEATURED WALLETS

Owner address	0x0000000000000000000000000000000000000000 **Ownership is renounced** *Original owner: 0xf010c756f4ea4ab1ea35823b3f42631433d9a0d3*
Marketing wallet	0x807970F5d3e76DB1EcE3Bd66c4C5F84Ad5894803
Development wallet	0xf010C756F4Ea4aB1eA35823b3F42631433d9A0d3
LP address	**Uniswap:** 0x5df597e24652c4c106605da3ae599a04906cfb91

TOP 3 UNLOCKED WALLETS

1 **3.4%** 0x4692304ed33df7fb7a5806f2485227b6c6c8d7d5

0xca4f451c70595de8035edbf0e773c6ac62dd14a6 **3.1%** 2

3 **3.01%** 0xf0fc584290a71830eb8b6b46f5b863ca85444153

VULNERABILITY CHECK

Design Logic	Passed
Compiler warnings.	Passed
Private user data leaks	Passed
Timestamp dependence	Passed
Integer overflow and underflow	Passed
Race conditions and reentrancy. Cross-function race conditions	Passed
Possible delays in data delivery	Passed
Oracle calls	Passed
Front running	Passed
DoS with Revert	Passed
DoS with block gas limit	Passed
Methods execution permissions	Passed
Economy model	Passed
Impact of the exchange rate on the logic	Passed
Malicious Event log	Passed
Scoping and declarations	Passed
Uninitialized storage pointers	Passed
Arithmetic accuracy	Passed
Cross-function race conditions	Passed
Safe Zeppelin module	Passed
Fallback function security	Passed

THREAT LEVELS

When performing smart contract audits, our specialists look for known vulnerabilities as well as logical and access control issues within the code. The exploitation of these issues by malicious actors may cause serious financial damage to projects that failed to get an audit in time. We categorize these vulnerabilities by the following levels:

High Risk

Issues on this level are critical to the smart contract's performance/functionality and should be fixed before moving to a live environment.

Medium Risk

Issues on this level are critical to the smart contract's performance/functionality and should be fixed before moving to a live environment.

Low Risk

Issues on this level are minor details and warning that can remain unfixed.

Informational

Information level is to offer suggestions for improvement of efficacy or security for features with a risk free factor.

FOUND THREATS

⚠ High Risk

Development wallet and marketing wallet can initiate manual token swaps from contract and withdraw eth from the contract.
If contract's token swap balance is 0 transactions will fail.

```
function manualswap() external {
    require(_msgSender() == _developmentAddress || _msgSender() == _marketingAddress);
    uint256 contractBalance = balanceOf(address(this));
    swapTokensForEth(contractBalance);
}

function manualsend() external {
    require(_msgSender() == _developmentAddress || _msgSender() == _marketingAddress);
    uint256 contractETHBalance = address(this).balance;
    sendETHToFee(contractETHBalance);
}
```

Informational

Before ownership renouncement owner could:
Enable/disable trading, blacklist address from trading.
Set fees without limit, set max transaction amount without limit.

```
function setTrading(bool _tradingOpen) public onlyOwner {
    tradingOpen = _tradingOpen;
}

function blockBots(address[] memory bots_) public onlyOwner {
    for (uint256 i = 0; i < bots_.length; i++) {
        bots[bots_[i]] = true;
    }
}

function setFee(uint256 redisFeeOnBuy, uint256 redisFeeOnSell,
uint256 taxFeeOnBuy, uint256 taxFeeOnSell) public onlyOwner {
    _redisFeeOnBuy = redisFeeOnBuy;
    _redisFeeOnSell = redisFeeOnSell;

    _taxFeeOnBuy = taxFeeOnBuy;
    _taxFeeOnSell = taxFeeOnSell;
}

function setMaxTxnAmount(uint256 maxTxAmount) public onlyOwner {
    _maxTxAmount = maxTxAmount;
}
```

Contract’s ownership is renounced.
Owner do not have any special privileges.

RECOMMENDATIONS FOR

GOOD PRACTICES

1. Consider fundamental tradeoffs
2. Be attentive to blockchain properties
3. Ensure careful rollouts
4. Keep contracts simple
5. Stay up to date and track development

GEISHA

GOOD PRACTICES FOUND

- ✔ The owner cannot mint new tokens after deployment
- ✔ The owner cannot stop or pause the contract
- ✔ The owner can set a transaction limit, but can’t lower it than 1% of total supply
- ✔ The smart contract utilizes "SafeMath" to prevent overflows

There is no information about the initial token distribution in their website and/or whitepaper.

TOKENOMICS

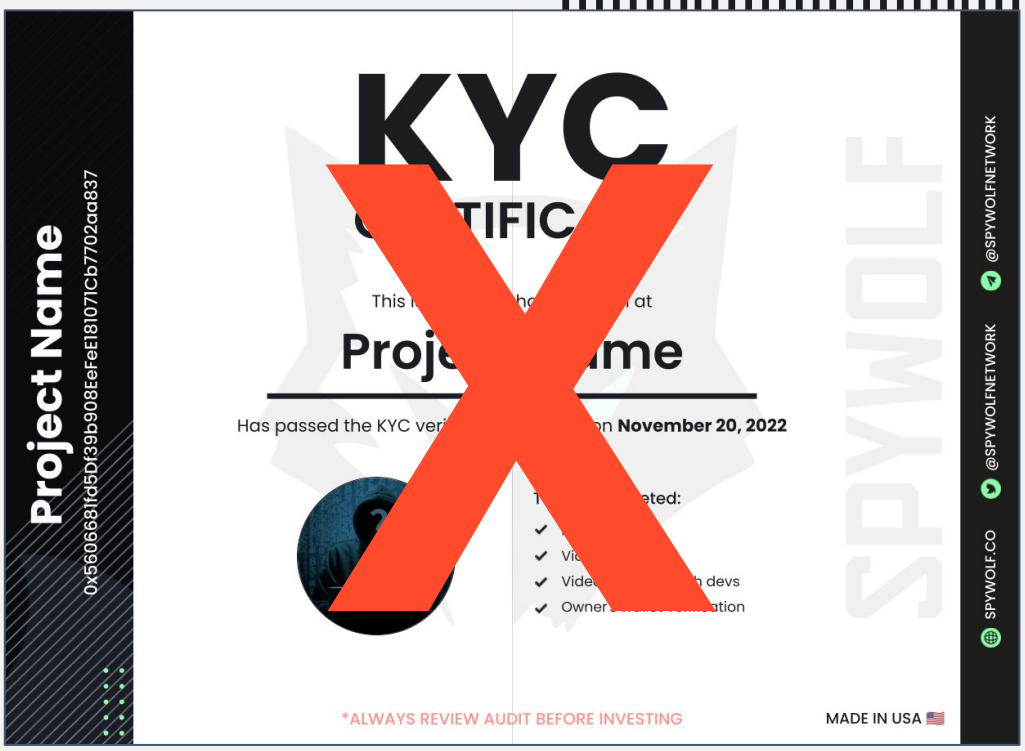
THE TEAM

⚠️ The team is annonymous

KYC INFORMATION

⚠️ No KYC

We recommend the team to get a KYC in order to ensure trust and transparency within the community.



WEBSITE

Website URL
http://geishaerc.com/

Domain Registry
https://www.godaddy.com

Domain Expiration
2023-12-29

Technical SEO Test
Passed

Security Test
Passed. SSL certificate present

Design
Simple but nice color scheme and overall layout.

Content
There is a lack of information about specific plans or strategies to be executed in this project.

Whitepaper
Not found

Roadmap
Yes

Mobile-friendly?
Yes

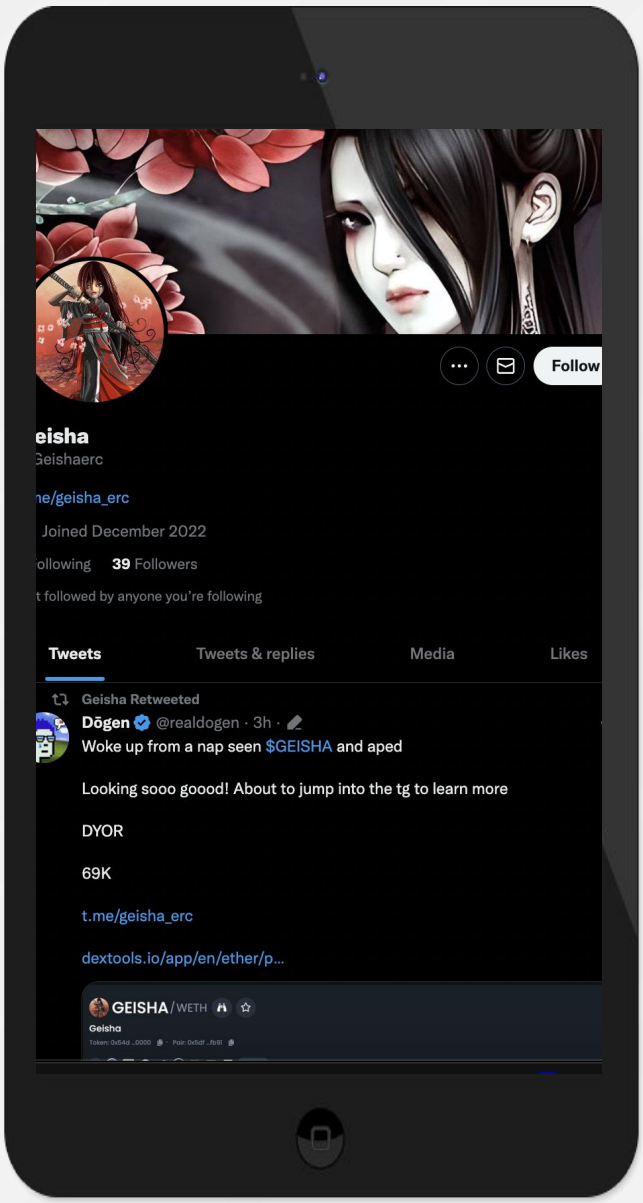
geishaerc.com

SOCIAL MEDIA

& ONLINE PRESENCE

ANALYSIS

The project's social media presence is new but active.



Twitter

@TwitterUSERNAME

- 39 followers
- Daily posts

Discord

Discord link here

- Not available

Telegram

@geisha_erc

- 98 members
- Active mods and devs
- Daily announcements

Medium

Medium link here

- Not available

SPYWOLF

CRYPTO SECURITY

Audits | KYCs | dApps
Contract Development

ABOUT US

We are a growing crypto security agency offering audits, KYCs and consulting services for some of the top names in the crypto industry.

- **OVER 150 SUCCESSFUL CLIENTS**
- **MORE THAN 500 SCAMS EXPOSED**
- **MILLIONS SAVED IN POTENTIAL FRAUD**
- **PARTNERSHIPS WITH TOP LAUNCHPADS, INFLUENCERS AND CRYPTO PROJECTS**
- **CONSTANTLY BUILDING TOOLS TO HELP INVESTORS DO BETTER RESEARCH**

To hire us, reach out to
contact@spywolf.co or
t.me/joe_SpyWolf

FIND US ONLINE

SPYWOLF.CO

SPYWOLF.NETWORK

@SPYWOLFNETWORK

@SPYWOLFOFFICIAL

@SPYWOLFNETWORK

@SPYWOLFNETWORK

Disclaimer

This report shows findings based on our limited project analysis, following good industry practice from the date of this report, in relation to cybersecurity vulnerabilities and issues in the framework and algorithms based on smart contracts, overall social media and website presence and team transparency details of which are set out in this report. In order to get a full view of our analysis, it is crucial for you to read the full report.
While we have done our best in conducting our analysis and producing this report, it is important to note that you should not rely on this report and cannot claim against us on the basis of what it says or doesn't say, or how we produced it, and it is important for you to conduct your own independent investigations before making any decisions. We go into more detail on this in the disclaimer below – please make sure to read it in full.

DISCLAIMER:
By reading this report or any part of it, you agree to the terms of this disclaimer. If you do not agree to the terms, then please immediately cease reading this report, and delete and destroy any and all copies of this report downloaded and/or printed by you. This report is provided for information purposes only and on a non-reliance basis, and does not constitute investment advice.
No one shall have any right to rely on the report or its contents, and SpyWolf and its affiliates (including holding companies, shareholders, subsidiaries, employees, directors, officers and other representatives) (SpyWolf) owe no duty of care towards you or any other person, nor does SpyWolf make any warranty or representation to any person on the accuracy or completeness of the report.
The report is provided "as is", without any conditions, warranties or other terms of any kind except as set out in this disclaimer, and SpyWolf hereby excludes all representations, warranties, conditions and other terms (including, without limitation, the warranties implied by law of satisfactory quality, fitness for purpose and the use of reasonable care and skill) which, but for this clause, might have effect in relation to the report. Except and only to the extent that it is prohibited by law, SpyWolf hereby excludes all liability and responsibility, and neither you nor any other person shall have any claim against SpyWolf, for any amount or kind of loss or damage that may result to you or any other person (including without limitation, any direct, indirect, special, punitive, consequential or pure economic loss or damages, or any loss of income, profits, goodwill, data, contracts, use of money, or business interruption, and whether in delict, tort (including without limitation negligence), contract, breach of statutory duty, misrepresentation (whether innocent or negligent) or otherwise under any claim of any nature whatsoever in any jurisdiction) in any way arising from or connected with this report and the use, inability to use or the results of use of this report, and any reliance on this report. The analysis of the security is purely based on the smart contracts, website, social media and team.
No applications were reviewed for security. No product code has been reviewed.